

MASTER SOFTWARE AS A SERVICE (HOSTING) AGREEMENT

THIS MASTER SOFTWARE AS A SERVICE (HOSTING) AGREEMENT ("Agreement") is entered into as of **September 29, 2017** (the "Effective Date"), by and between TE Connectivity Corporation, a Pennsylvania Corporation, on behalf of itself and including its global affiliates and other companies wholly owned or controlled, directly or indirectly, or under common control with TE Connectivity Ltd. ("TE") and Convercent, Inc., a Delaware Corporation, with an office located at 929 Broadway, Denver, CO 80203 ("Supplier"). TE and Supplier are individually hereinafter referred to as a "Party" and collectively as the "Parties".

WITNESSETH; That

WHEREAS, Supplier desires to provide to TE, and TE desires to obtain from Supplier certain services according to the terms and conditions set forth herein; and

NOW, THEREFORE, for and in consideration of the agreements set forth herein, TE and Supplier agree as follows:

I. SCOPE

- (A) Services. Pursuant to the terms of this Agreement, Supplier shall provide TE with products and modules provided via a Supplier website and/or mobile application, all user documentation, information and materials contained within such products or modules, and related support, professional services and other services provided by Supplier, including but not limited to training of the new Supplier offerings, and transition and implementation services associated with migrating from TE's prior system to the Supplier offerings (the "Services") as explicitly identified Appendix C, and/or in one or more Order Forms and/or in accordance with the specifications provided within a "Statement of Work" or "SOW" that is agreed to and executed by the Parties. The invalidation, fulfillment, waiver, termination, or any other disposition of any rights or obligations of either TE or Supplier or both, arising from the execution of this Agreement in conjunction with any one Statement of Work shall not affect the status of the rights or obligations of either or both of the parties arising from the execution of this Agreement in conjunction with any other Order Form or Statement of Work. Additional Order Forms or Statements of Work may be executed from time to time by TE and Supplier and if the Order Forms or Statements of Work refer by date to this Agreement, they shall be subject to the terms and conditions of this Agreement regardless of the date they are executed, notwithstanding that a prior period of effectiveness of this Agreement may have lapsed through expiration or termination of all Statements of Work previously executed pursuant to this Agreement
- (B) Purchase Orders. The Parties further agree and acknowledge that this Agreement is being executed in conjunction with one or more "Purchase Orders" which, by specific reference to this Agreement and upon execution by TE and acceptance by Supplier, become subject to all of the terms and conditions contained in this Agreement. For purposes of this Agreement, Purchase Order shall mean the commercial document issued by TE and referencing the Order Form and sent to Supplier for governance of services and expenses. In the event of any conflict between the terms of this Agreement, the Statement or Work and/or Order Form and the Purchase Order, the order of precedence shall be: (1) terms in the Statement of Work, (2) terms specified on the face of a Order Form and/or Purchase Order, and (3) the terms of this Agreement. For

clarity, any standard terms associated with a TE purchase order, or Supplier Order Form shall not be binding on the parties, other than those terms referenced to within this Agreement.

- (C) Time is of the Essence: TIME IS OF THE ESSENCE IN SUPPLIER'S PERFORMANCE OF ITS OBLIGATIONS IN RELATION TO ITS IMPLEMENTATION OBLIGATIONS SET FORTH IN THE STATEMENT OF WORK DATED SEPTEMBER 27, 2017. Supplier shall promptly notify TE in the event Supplier, for any reason, anticipates difficulty in complying with the required Statement of Work or in meeting any of TE's requirements.
- (D) Record Retention. Supplier shall maintain accurate and complete records evidencing its compliance with this Agreement and the Services performed hereunder ("Records"). All Records shall be available, at TE's expense, for inspection, copying, and audit by TE or its designee during Supplier's normal business hours upon reasonable notice, once per year, for a period of six (6) years after the completion, expiration or termination of this Agreement, for the purpose of verifying Supplier's compliance with the terms hereof and applicable law; provided however, nothing herein shall prevent TE from obtaining necessary records to respond to any governmental request, subpoena or legal proceeding.
- (E) No Exclusivity. The Parties agree that this Agreement is not exclusive and that TE has the right at its discretion at any time to engage other parties to perform services of a similar nature.

II. TERM & TERMINATION

- (A) Term. The term of this Agreement shall commence on the Effective Date and continue for a period of five (5) years, unless earlier terminated by either Party as set forth herein (the "Term").
- (B) Termination for Convenience. Eighteen (18) months after the Effective Date, TE may terminate this Agreement at any time, without cause, upon one hundred eighty (180) days prior written notice to Supplier. TE shall accelerate payment of all unpaid amortized fees relating to "Premium Implementation" and "Data Migration and related support," as detailed in the applicable Statement of Work or Order Form at time notice of early termination was delivered to supplier, with fees to be paid by the date of termination.
- (C) Termination for Cause. Either Party may terminate this Agreement, any Statement of Work or Order Form for cause, immediately and without prior written notice, in the event of any of the following:
 - (1) a breach of any covenant, representation or warranty hereunder, that, if curable, is not cured within thirty (30) days following receipt of written notice thereof;
 - (2) a failure to fulfill or perform any duties or obligations pursuant to this Agreement, provided that the breaching Party fails to remedy any such failure within fifteen (15) days of its receipt of a written notice from the non-breaching Party outlining the breaching Party's failure;

- (3) in the event that (i) any change in the active management or ownership of Supplier or (ii) the sale, transfer or other disposition of all or substantially all of the assets of Supplier or any affiliate, division or unit of Supplier that is performing Services hereunder, results in Supplier competing with TE, TE may Terminate this agreement immediately; or
- (4) if (i) any proceeding in bankruptcy, reorganization or arrangement for the appointment of a receiver or trustee to take possession of the other Party's assets or any other proceeding under any law for relief from creditors shall be instituted by or against the other Party (and such proceeding is not dismissed within sixty (60) days from the filing date); or (ii) if the other Party shall make an assignment for the benefit of its creditors.
- (D) Effect of Termination. The termination of this Agreement shall automatically terminate all outstanding Statements of Work, Order Form, and/or Purchase Orders. The termination of a Statement of Work, Order Form, and/or Purchase Order will not be deemed a termination of this Agreement. Upon termination of this Agreement, or an applicable Statement of Work, Order Form, and/or Purchase Order, the rights and licenses granted thereunder shall cease and the Services will immediately terminate. After receipt of a notice of termination, and except as directed by TE, (a) Supplier shall immediately: (i) stop work as directed in the notice; (ii) place no further subcontracts or orders for materials, services, or facilities, except as necessary to complete the continued portion of the Agreement, if any; and (b) Supplier shall promptly: (iii) terminate all subcontracts to the extent they relate solely to Services terminated; (iv) destroy or return to TE all actual and potential client and contact lists, all information, whether in printed or electronic form – if in electronic form, then returned in an acceptable and readable format by TE, and all films, tapes, computers, documents, reports, evaluations, plans, specifications, drawings, programs, worksheets and materials furnished to Supplier by TE or developed by Supplier in performing the Services, and Supplier will not make or retain any copies or excerpts of such information or materials; and (v) deliver to TE all works and Deliverables completed through the termination date. After termination, Supplier shall submit a final termination settlement to TE for all work performed up to termination of this Agreement. Supplier will only be paid for services rendered and expenses incurred prior to the date this Agreement is terminated. In the event that this Agreement, a Statement of Work or Change Order is terminated by TE for cause, Supplier shall remit, within ninety (90) days, to TE a pro-rata refund of all Fees paid for any unused term of the Services. The terms and provisions of this Agreement, other than the terms and conditions for the continuation of performance and payment of Services, shall survive any termination or expiration of this Agreement.
- (E) Upon TE's request, following expiration or termination of this Agreement or any related Statement or Work, Supplier shall, unless otherwise agreed by the parties, scrub all digital TE information in its possession from its computers and servers, or computers and servers of any third party (including but not limited to a hosting facility) in such a manner as to make it unreadable (with the exception of encrypted backups, which have a 365 day retention period). For clarity, Supplier shall not scrub any digital TE information without first receiving express written approval of such action from TE, provided however, no sooner than ninety (90) days following termination, Supplier shall scrub all digital TE

information from any production servers. Upon request, Supplier shall certify that all data has been scrubbed from its servers in accordance with this section.

III. PAYMENTS AND INVOICING

- (A) Invoices. Subsequent to the execution of this Agreement, Supplier will gain access to TE's designated supplier management system at www.te.com ("TE Supplier Portal"). Supplier shall submit all invoices through the TE Supplier Portal. To be valid and eligible for payment, invoices must include, among other things, the Purchase Order number unique to the project and provided by TE.
- (B) Designated Fees. In consideration of Supplier providing the Services, TE shall pay to Supplier the fees set forth in the applicable Statement of Work, Order Form and/or Purchase Order (the "Fees"). As indicated in Supplier's Order Form, Supplier's fees do not include any taxes, levies, duties or similar governmental assessments of any nature (collectively, "Taxes"). TE is responsible for paying all Taxes associated with its purchases hereunder, excluding taxes on Supplier's net income. If Supplier has the legal obligation to pay or collect Taxes for which TE is responsible under this Agreement, Supplier will invoice TE and TE will pay that amount unless TE provides Supplier a valid tax exemption certificate from the appropriate taxing authority. Supplier shall provide invoices of the Fees on a per project basis detailing the nature of the services performed, the rate at which the services were performed and the expenses, if any, that were incurred. TE will pay Supplier for all services rendered and approved expenses within thirty (30) days after receipt of Supplier's invoice, expense receipts and expense voucher. The making of any payment or payments by, or on the behalf of, TE shall not imply acceptance by TE of such items or the waiver of any warranties or requirements of, or rights to make any claims under, this Agreement.
- (C) Additional Expenses. TE shall reimburse Supplier for all authorized reasonable and actual out-of-pocket expenses incurred by Supplier in connection with the Services provided, however, that any such expenses shall be approved by TE, in writing, prior to Supplier incurring any such expense and provided Supplier submits receipt for expenses no later than thirty (30) days following the end of the month in which the expenses were incurred. Unless agreed otherwise, Supplier shall utilize personnel local to the area in which the Services are performed ("Local Personnel") whenever possible to minimize travel and living expenses incurred. Travel and living expenses charged to TE under this Agreement shall be consistent with TE's then current travel policy (currently, which may be found on the TE Supplier Portal). When Supplier personnel visit more than one client on the same trip, the expenses incurred are apportioned in relation to time spent with each client. Supplier shall use commercial reasonable efforts to make all reservations sufficiently in advance of the travel date so as to obtain the lowest price possible.
- (D) Rights of Set-Off; Disputed Amounts. With respect to any amount that (i) should be reimbursed to TE or (ii) is otherwise payable to TE pursuant to this Agreement or a Statement of Work, TE may deduct the entire amount owed to TE against the Fees or against the expenses owed by TE to Supplier under this Agreement, Order Form, or Statement of Work. Any unused credits against future payments owed to TE shall be paid to TE within thirty (30) days after the termination or expiration of this Agreement or the relevant Statement or Work. Further, TE shall have the right to withhold payment of any amount due to

Supplier that TE reasonably disputes in good faith, which shall not constitute a material breach of this Agreement or TE's payment obligations.

- (E) This section has been intentionally deleted.
- (F) Waiver of Billing. TE shall not be liable for, and Supplier shall waive its right to claim payment of, any fees, costs, taxes and expenses arising out of this Agreement for which TE does not receive an invoice within ninety (90) days after the date such invoice should have been provided to TE in accordance with this Section III.
- (G) Credits. Any amount that (i) should be reimbursed to TE or (ii) is otherwise payable to TE pursuant to this Agreement, Order Form, or a Statement of Work, TE may deduct the entire amount owed to TE against the fees shall be paid to TE within thirty (30) days of TE's claim for payment of such credit.
- (H) Fee Adjustments. The fees charged for a particular product or service are fixed, and shall not increase during the subscription period referenced in the SOW, Order Form, or Purchase Order (or similar document).

IV. CONFIDENTIALITY AND DATA PROTECTION

- (A) Confidential Information. Pursuant to the Services to be rendered hereunder, each Party now has or will have possession of or access to information relating to the other that is, or should be reasonably understood to be, confidential or proprietary information of the other, disclosing, Party, whether disclosed orally or in writing by any other media. Provided, however, that TE has the express right and ability upon termination or expiration of this Agreement to share reports and similar output related formats and data to prospective replacement vendors so TE can ensure continuity of information and reporting. All such information, other than any information developed independent from the disclosing Party's information, that is in the public domain or previously known to the recipient of the information through no act or omission of either Party, or which it is authorized to disclose, is hereinafter referred to collectively as the "Confidential Information." Each Party agrees to hold secret and protect the other Party's Confidential Information and use that degree of care that it uses or would use with respect to its own proprietary and confidential information to keep the Confidential Information secret. Further, each Party agrees to: (i) refrain from using the other Party's Confidential Information except as contemplated herein; and (ii) not disclose such Confidential Information to any third party except to contractors or representatives as is reasonably necessary in connection with this Agreement (and only subject to binding use and disclosure restrictions at least as protective as those set forth herein executed in writing by such contractors or representatives). The Parties shall return to the other, or destroy and certify the destruction thereof, all Confidential Information and reproductions thereof that are in its possession immediately upon request, including upon the expiration or termination of this Agreement. For the avoidance of doubt, Confidential Information shall include the terms of this Agreement; all data and information loaded, processed and/or stored in the Service as well as all information pertaining to products, processes or business operations; confidential information pertaining to either Party's customers and prospective customers, customer requirements, customer financial information and other such confidential information compiled or maintained internally by either Party covering its' customers and prospective customers; and confidential information pertaining to

either Party's sources of supply, costs, marketing plans, and contemplated activities, product design, and other such confidential information compiled or maintained internally by either Party concerning its business operations and activities including but not limited to all information which is disclosed or made available by either Party, or which is observed by either Party, in connection with the Supplier's access to TE's Computer Systems. Marketing and financial information shall also be conclusively presumed to be Confidential Information unless publicly published in writing.

- (B) Upon termination of performance of services pursuant to any Statement of Work or Order Form issued pursuant to this Agreement, and upon TE's request, Supplier agrees to promptly return to TE, and/or at TE's election destroy and certify the destruction thereof, any and all documents containing any of the Confidential Information of TE referred to above, and not to make any written record of such information nor disclose such information to others nor to make any use of such information. Upon request, Supplier shall (i) make available and transfer to TE in a machine readable format or other methods to be mutually agreed by the parties, or TE's designated third party, all of TE's data stored by the hosted services in a mutually agreed upon format (via an SFTP site, for example), and (ii) take reasonable steps to assist with transfer of any dedicated phone numbers and other tools and mechanisms used by Supplier or its contractors in connection with the Service. Supplier shall destroy all copies of such data, and direct any subcontractors to destroy its copies of such data, no later than ninety (90) days after termination. Upon request Supplier will provide proof of destruction.
- (C) Each party acknowledges that this Agreement provides notice that the Parties each regard it to be vital to its respective interests that its Confidential Information be safeguarded. Each Party understands that this Agreement establishes a confidential relationship between the Parties and that each Party has a duty under the law not to breach the confidential relationship by using or disclosing Confidential Information of the other Party. The Parties further understand that each relies upon the other Party and its employees honoring such duty of confidence when entrusting such Party and its employees with access to its Confidential Information. Where such action does not violate applicable law, Supplier shall provide TE with notice if it receives a subpoena or other court or governmental order to disclose TE Confidential Information and Supplier will work cooperatively with TE to secure an appropriate protective order and/or limit the extent of the disclosure.
- (D) Data Protection. For the provision of the Services it may be necessary for TE to provide personal information (also referred to as "personal data", which is any information relating to an identified or identifiable natural person, or as otherwise defined by applicable law). A TE entity will do this on its own behalf or also on behalf of its global affiliates. As a data processor Supplier will comply with any instructions of TE, keep the personal information confidential and secure and only use the personal information for rendering the Services and not share the confidential or personal information with any third party without the prior written approval of TE. TE's personal information can also be Confidential Information as described above.

Supplier will comply with any data protection laws that may apply on the processing by Supplier of personal information of TE such as, but not limited to, the EU data protection directive 95/46 and the new EU General Data Protection Regulation 2016-679 that will replace this directive as of May 25, 2018.

1. International transfers. Coincident with executing this Agreement TE and Supplier will execute the attached "Exhibit on the processing of personal information" (Appendix A), which includes the EU Standard Contractual Clauses. This will be required in case TE will have to transfer personal information originating from TE Connectivity Corporation affiliates in countries, such as but not limited to those of the European Economic Area, that have restrictions on the transfer of personal information to countries that do not have laws that provide adequate protection of personal information. Review whether this may apply the "Privacy exhibit checklist" on <https://supplier.te.com/web/supplier-portal/home>.

Because Supplier has certified its compliance with the Privacy Shield, by which it commits to apply with the relevant data protection principles in its capacity as a data processor, Appendix A will only apply as of the moment the Supplier's Privacy Shield would no longer be valid or when the adequacy decision for the Privacy Shield program would be annulled. This also requires that Supplier will continue to be certified for the Privacy Shield during the course of this Agreement or any longer period of time when Supplier would still retain personal information of TE and informs TE when Supplier's certification for the Privacy Shield would no longer be valid.

2. Access controls and training. Supplier shall establish a procedure for identifying its users who have access to TE personal information. Supplier will ensure that any Supplier employee to whom any TE personal information is disclosed has received appropriate data protection training and is made aware of the requirements of this Agreement and of the confidential nature of TE personal information and require such employees to comply with this Agreement and any other obligations required pursuant to applicable data protection laws. Upon request, Supplier shall provide TE with the name and contact details of its data protection officer.

Supplier will work with TE to allow individuals (data subjects) to enforce their legal rights to access their personal information, have it corrected, updated or deleted.

3. Security incident. Supplier will inform TE without undue delay and, where feasible, not later than 48 hours after having become aware of it (in line with time limits set by applicable law) about any security incident that compromises the security, confidentiality or integrity of the personal information of TE as processed by Supplier ("personal data breach"). Supplier will render TE all reasonable assistance in order to allow TE to comply with its obligations under data breach notification laws. In case the data breach is caused by non-compliance of Supplier with its contractual commitments, Supplier shall compensate TE for all costs related with containing and managing the consequences of the data breach. This may include, but is not limited to, costs of notification and legal fees incurred by TE.

Security incident means any unauthorized action by a known or unknown third party which, whether successfully completed, attempted or threatened, should reasonably be considered to constitute one of the following with regard to the Service or TE: an attack, penetration or denial of service; unauthorized access to or disclosure of data or Confidential Information of TE or its customers; misuse of the Service or software access or intrusion (hacking) to the Service or software; virus intrusion of the Service or

software; scan of the Service, or any other activity that could affect TE data or TE Confidential Information.

4. **Audit.** Supplier will conduct an annual internal data privacy review to check its compliance with the contractual and legal requirements. Supplier employees who process TE personal information will only do so in compliance with this Agreement, instructions provided by TE, and in conformity with applicable law. Upon request, TE will receive access to the internal compliance reviews. Once per year, TE shall have the right to have reasonable access, upon prior written notice, to check compliance with the technical and security measures implemented to protect TE personal information and to inspect the premises, facilities and IT systems used by Supplier for this purpose and proper compliance with this Agreement in general. Supplier will provide its reasonable cooperation with such audits.
5. **Subcontracting.** Supplier may not, without the prior written notice to TE, subcontract data processing for the Services to third parties, including affiliates that are located in countries that, according to the EU, do not have laws that provide adequate protection. TE shall have sixty (60) days' after receiving written notice from Supplier in which to determine in its commercially reasonable discretion whether such a subcontractor provides viable security; Approval can only be provided by TE when the subcontractor (sub-processor) will be contractually bound to provide a level of protection of TE's personal data that is comparable to what Supplier must provide which has to be reflected in Appendix A. This may require the subcontractor to be contractually bound to comply with the Standard Contractual Clauses or another legal basis that may apply in future for data transfers from countries that have transfer restrictions as to be specified in Appendix A. Supplier remains liable for the proper performance of the Services by its subcontractor.

TE hereby consents to the Supplier's use of the followings subcontractors (sub-processors) as set out below:

Subprocessor	Brief Description of Processing
Five Star Call Centers	Call Center – Helpline/Call Center Services
Amazon Web Services	Data Center – Failover Cloud Environment
Microsoft Azure	Data Center – Primary Cloud Environment
Datavail	Database Administration – 24/7 Database Monitoring
Bing	Automated translation services built into the Services
Lionbridge	Professional translation services outside the Services

6. **Security standards.** Supplier's product is ISO 27001:2013 certified and

Supplier shall maintain such certification throughout the Term, and shall provide TE with a copy of Supplier's certification of compliance.

7. Non-compliance. Supplier will notify TE as soon as it determines that it can no longer comply with the data security measures to be applied in conformity with this Agreement or the Privacy Shield as far as applicable. Upon receiving such notice TE will promptly take such reasonable steps that are required to safeguard the continued proper protection of the personal information which may include the discontinuation of the sharing of personal information with the Supplier until the issue has been resolved.
 8. Government access. Supplier will promptly notify TE of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority that it receives and which relates to TE's personal information that Supplier processes unless that would conflict with applicable law. Supplier will inform TE upon its request about any further details about the order, as far as it possesses such information and will provide reasonable assistance to TE to comply with such order within the applicable time limit.
 9. Data portability. Following termination of the Agreement, upon TE's request, Supplier will return to TE or its agent, or destroy and certify the destruction thereof, all TE's personal information and/or Confidential Information that it processes or make this available to TE or its agent in a mutually agreeable format. Following the return of the personal information, or as otherwise specified in an agreement, Supplier will promptly delete or otherwise render inaccessible and unreadable (e.g. scrubbed from any and all computers) all copies of TE's personal information from the systems it used for rendering the Services (with the exception of encrypted backups, which have a 365 day retention period).
 10. Changes in applicable law. In the event there will be changes in the applicable data protection laws, the Parties agree to work cooperatively to make any necessary modifications to this Agreement in order to comply with such changes.
- (E) Subcontractors – Supplier confirms that it has appropriate confidentiality obligations in place with any of its subcontractors who will perform services for TE, including but not limited to the call-center that may handle incoming phone calls from a hotline system, and Subcontractors are bound to a code of conduct substantially similar to that of both Convercent and TE.
- (F) Remedy. Each Party hereby acknowledges that disclosure of the Confidential Information by it or breach of the provisions contained herein will give rise to irreparable injury to the other Party and such breach or disclosure is inadequately compensable in money damages. Accordingly, each Party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings. Such remedy shall not be deemed to be the exclusive remedy for any such breach but shall be in addition to all other remedies available at law or equity. Each Party hereby further acknowledges and agrees that the covenants contained herein are necessary for the protection of the other Party's legitimate business interests and are reasonable in scope and content.
- (G) Insider Trading. TE's Confidential Information may constitute material inside information under the securities laws of the United States, and use of this information to trade in the securities of TE Connectivity Ltd., or sharing the

information with others who trade in the securities of TE's parent is a violation of this Agreement and may be a violation of law.

- (H) No Publicity. Except as specifically authorized in writing by TE, Supplier shall not use any identification of or reference to any trade name, trademark, service mark, service name or symbol of TE in any advertising or promotional efforts, nor disclose that it is performing Services hereunder, or any information, materials, reports, and other work product that Supplier creates or develops as part of the Services.

V. SOFTWARE AS A SERVICE (HOSTING)

The Services and all components thereof are licensed, not sold. Supplier and its suppliers exclusively own and retain all rights, title, and interest in and to the Services (including software, user interface designs, and documentation) and all additions and modifications to the Services, including all intellectual property rights therein. Subject to the terms and conditions of this Agreement, during the term, Supplier will provide, to or on behalf of TE, the Services components specified in the applicable Order Form or SOW, provided that, with respect to provision of all subscription-fee-based Services, the Customer Number does not increase compared to the Customer Number (a) specified in the applicable Order Form or SOW or (b) subsequently agreed to by the parties as the applicable Customer Number. "Customer Number" means the total number of employees and contract employees of TE and all its affiliates. TE represents the initial Customer Number specified on each Order Form or SOW is accurate. Supplier may request and TE shall provide the then-current Customer Number from TE prior to each anniversary of the Effective Date.

- (A) Software as a Service (Hosting) Application. If, as part of the Agreement, Supplier will provide TE with remote access and hosting of the software across the Internet, including a browser interface, access, storage, transmission and distribution ("Hosting Services"), then Supplier shall host the software through its subcontractors, as of the Effective Date, Microsoft Azure in Dublin, Ireland and Amazon Web Services in Frankfurt, Germany. Supplier shall be responsible for hosting, supporting and maintaining the infrastructure required to host the software for TE. TE will have access to the software via the Internet at the designated web site or IP address provided to TE by Supplier. TE shall be responsible for obtaining and maintaining its connection to the Internet. In the event that Supplier relocates its data center, Supplier shall provide to TE the data center's updated address within two (2) weeks. Notwithstanding the foregoing, Supplier shall not move its data center, or any servers performing hereunder, outside the country of the originally approved location without the consent of TE, which shall not be unreasonably withheld.
- (B) System Availability.
1. Web Application. Supplier will maintain 99.8% uptime of the web based Services (the "Web Application SLA"). The calculation of uptime will exclude scheduled downtime. Supplier will inform TE reasonably in advance of any scheduled downtime. Scheduled downtime will occur, as needed, outside the normal business of 8:00 a.m. to 5:00 p.m. MT, Monday - Friday, excluding holidays, as modified from time to time by Supplier with advance written notice to TE.
 2. Call Center. To the extent applicable to Services ordered by TE pursuant to an Order Form, the call center shall be available to receive

telephonic reports in the event of an outage within the web application and 80% of TE's calls to the call center shall be answered in 20 seconds or less (the "Call Center SLA", which, along with the Web Application SLA is referred to as the "SLA"). To receive this SLA, TE's Order Form must include dedicated phone lines.

3. Remedy. Supplier's sole liability (and TE's exclusive remedy) for Supplier's breach of either or both SLAs shall be to issue a service credit ("Service Credit") for the applicable Services for the applicable month, in the amount specified in the table below. Such Service Credit shall be issued within thirty (30) days of written request by TE. In the event two SLA remedies apply, Supplier will provide a service credit for the higher amount.

Actual Web Application Service Level for the month (% of uptime)	Actual Call Center Service Level for the month (% of calls answered in 20 seconds or less)	Service Credit to be issued (% of TE service fees)
99.0 - 99.79%	75.0 – 79.99%	5%
98.0 – 98.99%	70.0 – 74.99%	10%
95.0 – 97.99%	65.0 – 69.99%	25%
90.0 – 94.99%	60.0 – 64.99%	50%
less than 90%	Less than 60%	100%

- (C) Additionally, a violation of the Web Application SLA below 90% and/or a violation of the Web Application SLA or Call Center SLA for three (3) consecutive months shall be considered a material breach of the Agreement and TE shall have the right to immediately terminate this Agreement with no further monetary obligation or liability.
- (D) Security. Supplier shall comply with the standards set forth in ISO 27001:2013, or equivalent standards that are (i) at least equal to industry practices for such types of locations, and (ii) which provide appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access of TE Data, User Information or Confidential Information.
- (E) Without limiting the provisions of Section (D) above, Supplier shall take all appropriate measures to secure and defend its location and equipment against "hackers" and others who may seek, without authorization, to modify or access Supplier's systems or the information found therein. Supplier will periodically, but in no event less than once per year, test its systems for potential areas where security could be breached. Supplier will promptly, and in any event within forty-eight (48) hours, report to TE any breaches of security or unauthorized access to Supplier's systems that Supplier detects or becomes aware of; such notification shall include when the breach occurred, whether it affected TE data, what TE data (if any) was affected, and what Supplier is doing (or has done) to address the breach. Supplier will use diligent efforts to remedy such breach of security or unauthorized access in a timely manner, but in no event shall the remedy take

longer than thirty (30) days, and, upon request, deliver to TE a root cause assessment and future incident mitigation plan with regard to any breach of security or unauthorized access affecting the software, TE or TE's Confidential Information. In addition, Supplier shall work cooperatively with TE to prepare any necessary response to the breach to the extent it affects TE or its supplier, customers or employees.

- (F) Beginning June, 2018, Supplier shall conduct SAS70 Type II or SSAE 16 audits and, upon request, provide the results to TE, and there shall be no significant findings or outstanding actions. Supplier shall have a written Disaster Recovery Plan. Upon request, Supplier shall provide TE with access to the Disaster Recovery Plan.
- (G) Supplier shall support TE with all reasonable requests related to electronic legal discovery associated with any claims or litigation in which TE is or may become a party.
- (H) Seat Parking. Supplier agrees that if the Hosted Services are priced and invoiced on a user count basis TE may set aside licenses of named or concurrent users, as applicable, which shall be deemed "inactive" users for a specified term during which TE shall not be obligated to pay annual user fees for such inactive users. During such inactive term, TE may notify Supplier in writing that it desires to reactivate all or a specified number of the inactive users. At the time of any such reactivation, Supplier will reactivate the users at the prices stated in Exhibit A. TE shall not be obligated to pay any retroactive fees applicable to such inactive users for the inactivation term.
- (I) Seat Transferability. Supplier acknowledges and agrees that TE shall be permitted to transfer user licenses among TE Connectivity Corporation's various affiliates irrespective of state, province, country or world region.
- (J) The software shall perform in compliance with the specifications and documentation provided by Supplier. Supplier shall not reduce or eliminate material features or functionalities of the Service during the term of the Agreement.
- (K) Outage and/or Disruption Reporting. As soon as practical after first becoming aware of any outage or disruption of the Service or material degradation of the software functionality, but in no case later than twenty-four (24) hours after first becoming aware thereof, Supplier shall report such outage, disruption or degradation to TE by email or telephone, as mutually agreed. Each such report shall include a summary of the effect of such outage, disruption or degradation and, if known, the cause thereof. As soon as practical after restoration of any such outage, disruption or degradation, but in no case later than twenty-four (24) hours after such restoration, Supplier shall report such restoration to TE by email or telephone, as mutually agreed.
- (L) TE hereby grants to Supplier and its authorized representatives and contractors a non-exclusive and non-transferable right and license to use, process, store, and transmit, and disclose TE data solely to provide the Services to TE and fulfill other obligations described in this Agreement. TE further authorizes Supplier to aggregate TE data with similar data from other Supplier customers in a manner that does not identify TE or include any Personal Information (defined below), to further develop the Services for Supplier customers.

VI. SUPPLIER'S REPRESENTATIONS AND WARRANTIES

- (A) Supplier represents and warrants that:
- (1) Supplier shall perform the Services hereunder in a professional and efficient manner, using due care, skill, diligence and at a level equivalent to the standards and practices of comparable companies in the industry, and acknowledges that its failure to perform the Services to this standard shall constitute a material breach of this Agreement;
 - (2) Supplier is not a party to any agreement that would prohibit Supplier from entering into this Agreement or fully performing the Services hereunder;
 - (3) Supplier has full right, title and authority to perform the Services and provide TE the rights to the Deliverables granted hereunder, and that the Deliverables are free of liens, encumbrances, claims or security interests of any kind;
 - (4) there is no outstanding, or threatened, litigation, arbitrated matter or other dispute to which Supplier is a party that would reasonably be expected to have a material adverse effect on Supplier's ability to fulfill its obligations under this Agreement;
 - (5) the Services and/or Deliverables do not impair or violate any copyright, trademark, patent, trade secret or other rights of any third-party, provided however that the sole and exclusive remedy for breach of this warranty shall be indemnification as provided in section VII below; and
 - (6) Supplier shall perform the Services hereunder in compliance with all applicable federal, state, county, and municipal statutes, laws, regulations, codes, ordinances and orders and Supplier shall obtain all applicable permits and licenses required in connection with its obligations under this Agreement.
 - (7) Its responses submitted to the TE Information Security Group in the Vendor Security Assessment are materially true and accurate as of the time of submission.
- (B) In the event that the Hosted Services include any software to be loaded onto TE's Computer Systems or require Supplier to have access to TE's Computer Systems, Supplier represents and warrants that it has used, and will continue to use, commercially reasonable measures to ensure that the Services do not contain any virus, malicious code, program or other internal component (e.g. Computer worm, computer time bomb or similar component) (hereinafter the "Harmful Code") which could (i) hinder TE's ability to use or benefit from the Services; (ii) in any manner, reveal, damage, destroy or alter any data or other information accessed through or processed by the Services or; (iii) in any manner, damage, destroy or alter TE's Computer Systems or data and other information accessed through or processed by TE's Computer Systems. Supplier shall immediately advise TE in writing upon reasonable suspicion or actual knowledge of such harmful code affecting TE.

VII. INDEMNIFICATION.

- (A) Indemnification. Supplier shall defend, indemnify and hold harmless TE, its parents and related entities, and their respective directors, officers, employees, shareholders and agents and all of their respective successors and permitted

assigns (the "TE Indemnified Parties"), from and against any and all third party suits, claims, actions, and causes of actions, and any liabilities, losses, damage to property or for injury to or death of any person, costs and expenses (including, but not limited to, interest, penalties, reasonable attorneys' fees and other expenses of litigation) associated thereto, arising from, or alleged to have arisen from:

- (1) the acts or omissions (whether negligent, reckless, intentional, or otherwise) of Supplier, its employees, agents, or independent Suppliers; and/or
- (2) any misrepresentation or breach of warranty by Supplier under this Agreement.

TE shall defend Supplier and its employees, officers, directors, shareholders, contractors, partners, members, owners, agents, predecessors, and permitted successors and assigns from and against any and all Claims (defined below) which allege any violation of applicable law by TE, other than any claims that would arise out of Supplier's own breach of their obligations, in connection with its use of the Services; or which relate to or are based on any event, claim or matter that is reported to TE via the Services. TE shall pay all costs of defense and all damages finally awarded or paid in settlement of any such Claim.

- (B) Infringement Indemnification. Notwithstanding any of the other indemnities or releases contained in this Agreement, Supplier shall indemnify, defend and hold the TE Indemnified Parties harmless from and against any and all third party claims, demands, suits, losses, and any causes of action of any kind whatsoever, and any liabilities, judgments, costs, expenses (including without limitation court costs, litigation expenses, and reasonable attorneys' fees), associated thereto (collectively referred to as "Claims") asserted by or arising in favor of any person or entity for or as a result of infringement or alleged infringement of any patents, copyrights, or trademarks, or misappropriation or misuse of any trade secrets or other confidential information, based on or related to the Services, Deliverables or Supplier, its subcontractors or agents, use or application of any processes, compositions, equipment, machines, articles of manufacture; or computer software. In connection therewith, Supplier shall at its sole expense and discretion either, (i) promptly undertake to procure for TE the right to continue using such Services and Deliverables or (ii) promptly replace or modify such Service or Deliverable to render it non-infringing but functionally equivalent. Provided that if (i) or (ii) are not available to or economically feasible for Supplier, then Supplier will have the right to terminate each affected Order Form or SOW and refund to TE the sums actually paid for using the Service or Deliverable and TE shall cease to use same.
- (C) Indemnification Procedure. Each party's indemnification obligation above is subject in each instance to the indemnified party (i) promptly giving notice of the claim to the indemnifying party; (ii) giving the indemnifying party sole control of the defense and settlement of the claim (provided that the indemnified party (including TE Indemnified Parties) shall have the right at their discretion and sole cost to be represented by its own counsel and to participate in the defense of any action in which any such a party is named as a party defendant, and the indemnified party's prior written approval will be required for any settlement that reasonably can be expected to require a material affirmative obligation of or, result in any ongoing material liability to such party; and (iii) providing to the indemnifying party all available information and reasonable assistance. The

remedies described above shall be the sole and exclusive remedy of the indemnified party and the sole obligation of the indemnifying party.

VIII. INSURANCE

- (A) Required Insurance. Prior to commencement of this Agreement, Supplier shall procure, and during the continuance of this Agreement shall maintain, at its sole cost and expense, insurance of the following kinds and amounts, or in the amounts required by law, whichever is greater. Supplier's procurement of such insurance shall in no way affect the indemnification or warranty provisions set forth in this Agreement, but shall be additional security therefore.
- (1) Workers' Compensation insurance prescribed by applicable local law;
 - (2) Employers Liability insurance with limits of at least \$1,000,000 for each accident;
 - (3) Comprehensive automobile liability covering all vehicles that Supplier hires or leases in an amount not less than \$1,000,000 (combined single limit for bodily injury and property damage);
 - (4) Comprehensive General Liability ("CGL") insurance including Contractual Liability Coverage covering the contractual obligations accepted under this section, with limits of at least \$2,000,000 for each occurrence of bodily injury, including death, and \$2,000,000 for each occurrence of property damage; and
 - (5) Technology – Errors & Omissions / Cyber Liability Insurance with limits of \$3,000,000 each claim.
- (B) Scope of Insurance. The automobile and CGL policies shall (i) name TE as an additional insured, including without limitation, with respect to third party claims or actions brought directly against Supplier or against TE and Supplier as co-defendants and arising out of this Agreement, (ii) contain a provision that TE, although named as an additional insured, shall nonetheless be entitled to recovery for any loss suffered by TE as a result of Supplier's negligence, (iii) include a waiver of subrogation in favor of TE, and (iv) be written as a primary policy not contributing with any other coverage which TE may carry. In the event that Supplier cannot obtain insurance as required above due to unavailability of such insurance products in Supplier's local market, then Supplier shall provide evidence of insurance that is comparable in scope and in amounts similar to those above or otherwise approved by TE in writing.
- (C) Certificates of Insurance. Supplier shall provide TE with certificates of insurance evidencing the required coverage, concurrently with the execution of this Agreement and upon request thereafter. Supplier shall not materially decrease or cancel the coverage above during the Term of this Agreement or for three (3) years thereafter. Such certificates shall be sent to the address as directed by TE.
- (D) Required Changes to Insurance. If said CGL policy does not automatically cover Supplier's contractual liability under this Agreement, Supplier shall obtain a specific endorsement adding such coverage. If said CGL policy is written on a "claims made" basis instead of a "per occurrence" basis, Supplier shall arrange for adequate time for reporting losses. Failure to provide contractual liability

endorsement coverage or adequate reporting time shall be at Supplier's sole risk.

- (E) Excess Liability. The insurance coverage's and limits specified herein shall not be construed in any way as limits of liability or as constituting acceptance by TE of responsibility for losses in excess of insurance coverage's or limits. No acceptance and/or approval of any insurance by TE shall be construed as relieving or excusing the Supplier from any liability or obligation imposed by the provisions of the Agreement.

IX. CONTINUED PROVISION OF SERVICES.

- (A) Force Majeure. If and to the extent that a Party's performance of any of its obligations pursuant to this Agreement is prevented, hindered or delayed by fire, flood, earthquake, elements of nature or acts of God, acts of war, strike, compliance with any law, regulation, or order of any governmental authority, or any other similar cause beyond the reasonable control of such Party (each, a "Force Majeure Event"), and such non-performance, hindrance or delay (i) could not have been prevented by reasonable precautions and (ii) does not arise as a result of such Party's breach of this Agreement, then the non-performing, hindered or delayed Party shall be excused for such non-performance, hindrance or delay, as applicable, of those obligations affected by the Force Majeure Event for as long as such Force Majeure Event continues and such Party continues to use its best efforts to recommence performance whenever and to whatever extent possible without delay, including through the use of alternate sources, workaround plans or other means. The Party whose performance is prevented, hindered or delayed by a Force Majeure Event shall promptly notify the other Party of the occurrence of the Force Majeure Event and describe in reasonable detail the nature of the Force Majeure Event.
- (B) No Payment for Unperformed Services. Except as otherwise provided for herein, nothing in this Article shall limit TE's obligation to pay any Fees; provided, however, that if Supplier fails to provide the Services in accordance with this Agreement due to the occurrence of a Force Majeure Event, the Fees shall be adjusted in a manner such that TE is not responsible for the payment of any Fees for those Services that Supplier fails to provide.
- (C) Allocation of Resources. If a Force Majeure Event or other similar extraordinary event causes Supplier to allocate limited resources between or among Supplier's customers, Supplier shall provide services to TE on at least an equal basis as to any other customers of Supplier in a similar pricing tier.

X. DISPUTE RESOLUTION.

- (A) Issue Escalation. Any issue between the parties that cannot be resolved by the Project Managers of both parties, shall (1) be brought to the attention of the next higher level of management of both parties, and if not resolved, (2) to the legal department of both parties prior to instituting Arbitration or litigation.
- (B) Continuity of Services. Supplier acknowledges that the timely and complete performance of its obligations pursuant to this Agreement is critical to the business and operations of TE. Accordingly, in the event of a dispute between TE and Supplier, Supplier shall continue to perform its obligations under this

Agreement in good faith, and TE shall continue to pay Fees therefor, during the resolution of such dispute unless and until this Agreement expires or is terminated in accordance with the provisions hereof.

XI. GENERAL PROVISIONS

- (A) Notices. All notices, requests, demands and other communications given hereunder (collectively, "Notices") shall be in writing and personally delivered or mailed by registered or certified mail, postage prepaid, return receipt requested to the below-referenced addresses, or to any other address designated by a Party in accordance with the provisions of this Section. All Notices shall be deemed delivered when actually received.

To TE:

TE Connectivity Corporation
TE Information Solutions
200 AMP Drive
P.O. Box 3608
Harrisburg, PA 17105

To Supplier:

Convercent, Inc.
Attn: Legal Department
929 Broadway
Denver, CO 80203

- (B) Social Responsibility. Supplier agrees to observe its Code of Conduct and, to the extent commercially practicably, the letter and spirit of TE's "Guide to Supplier Social Responsibility", current reference number TEC-1015, a copy of which may be obtained from TE upon request or at the TE Supplier Portal.
- (C) Anti-corruption. In fulfilling its responsibilities under this Agreement, Supplier and each of its owners, officers, directors, employees or agents (collectively and individually in this clause "Agent") must comply with its obligations under the law including without limitation, the Agent:
- (1) Must not violate any anti-bribery or anti-corruption law of any jurisdiction including the United States of America's Foreign Corrupt Practices Act and any country which is or becomes a signatory to the OCED Convention on Combating Bribery of Foreign Public Officials and in particular, the Agent must not pay, offer or promise to pay, or authorize the payment of, any monies or anything of value, directly or indirectly, to any government official or employee, any official or employee of a state-run or state-owned or controlled enterprise or entity, any official or employee of a public international organization, any candidate for political or public office, any official or employee of any political party, or any family member or relative of such persons or any political party for the purpose of influencing any act or decision of any such official, employee, candidate, political party, enterprise or entity, public organization, or government to obtain or retain business, or direct business to any person or entity, or for any other improper advantage or purpose, and

- (2) Shall fully comply with the Company's compliance and ethical conduct policies and programs on anti-bribery, attend training sessions as and when requested, and execute truthful compliance certificates whenever requested,

In the event the Agent breaches its obligations under this clause, or TE learns of or has a reasonable suspicion that the Agent has breached this clause or caused TE to violate the provisions of any law, notwithstanding any other provision to the contrary, TE may immediately terminate this Agreement and the Agent hereby waives any and all claims against TE for any loss, cost or expense, including, but not limited to, loss or profits, incidental or consequential damages, that Agent may incur by virtue of such termination of this Agreement.

- (D) Entire Agreement. This Agreement and all attachments hereto, all Statements of Work, all Order Forms, and all Purchase Orders issued hereunder and the Non-Disclosure Agreement between the parties, constitute the entire agreement between the parties hereto with respect to the transactions contemplated hereby, and supersede all written and verbal negotiations, representations, warranties, commitments, and other understandings prior to the date hereof between Supplier and TE. No shrink-wrap, click-wrap, or other terms and conditions or agreements ("Additional Terms") provided with any Services or Deliverables hereunder shall be binding on TE, even if use of such Services or Deliverables requires an affirmative "acceptance" of those Additional Terms before access is permitted. All such Additional Terms shall be of no force or effect and shall be deemed rejected by TE in their entirety. Appendices and other documents referred to in this Agreement are an integral part hereof, unless the context of such reference indicates otherwise.
- (E) Amendment and Waiver. This Agreement may be amended, and the observance of any term of this Agreement may be waived, only with the written consent of both Parties. Any waiver by either Party hereto of any provision of this Agreement shall not be construed as a waiver of any other provision of this Agreement, nor shall such waiver be construed as a waiver of such provision with respect to any other event or circumstance, whether past, present or future.
- (F) Execution in Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same agreement.
- (G) Assignment. Supplier will remain responsible for any Services that are subcontracted and for compliance with the terms and conditions of this Agreement. TE may assign this Agreement, without consent in the event of a change of controlling ownership interest (either directly or indirectly) in any TE entity or in the event of merger, recapitalization, consolidation, other business combination or sale of all or substantially all of the assets of any TE entity. Supplier may assign this Agreement to a successor who acquires substantially all of its assets or equity through purchase, merger or other change in control transaction without the TE's consent; provided however, within thirty (30) days following timely notice of such assignment, TE may terminate this Agreement in TE's sole discretion.
- (H) Acquisition. Supplier agrees that in the event TE Connectivity Corporation acquires a new business or divests, partially or wholly, of an affiliate, subsidiary or division which has licensed Supplier's Hosting Services, TE may assign to the newly acquired or divested entity the licensed Hosting Service or Named Users or Concurrent Users of the Supplier Hosting Service, as applicable after

notifying Supplier of the transaction. TE agrees that it may not assign the Hosting Service to a competitor of Supplier. Any such assignment shall require that the assignee of the licensed Hosting Service pays applicable user fees.

- (I) Governing Law. This Agreement shall be governed by and construed and enforced in accordance with the laws of the State of New York, United States of America, without regard to the conflict of laws principles thereof.
- (J) Dispute Discussion. Any claim or dispute arising out of this Agreement, except for a breach of the Confidentiality provisions hereunder, that has not been resolved using the issue escalation procedure set forth herein, shall be referred to and finally resolved by arbitration in New York, New York in accordance with the Rules of Arbitration of the International Chamber of Commerce by three (3) arbitrators appointed in accordance with the said rules. The language of the arbitration shall be English and all arbitrators shall be fluent in English.
- (K) Severability. If any provision or provisions of this Agreement shall, for any reason, be deemed unenforceable or in violation of law, such unenforceability or violation shall not affect the remaining provisions of this Agreement, which shall continue in full force and effect and be binding upon the parties hereto.
- (L) Section Headings. The headings of the sections, paragraphs, and appendices herein are for the Parties' convenient reference only and shall not define or limit any of the terms or provisions hereof.
- (M) Status of Parties. This Agreement shall not be construed as creating any agency, partnership, joint venture, or other similar legal relationship between the Parties; nor will either Party hold itself out as an agent, partner, or joint venture party of the other party. Both Parties shall be, and shall act as, independent suppliers. Neither Party shall have authority to create any obligation for the other Party, except to the extent stated herein.
- (N) Damages. EXCEPT WITH RESPECT TO CLAIMS RELATED TO BREACH OF CONFIDENTIALITY, BREACH OF SECURITY, IP INFRINGEMENT OR INDEMNIFICATION FOR THIRD PARTY CLAIMS, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LIABILITY FOR LOSS OF USE, LOSS OF PROFITS, LOSS OF PRODUCT OR BUSINESS INTERRUPTION HOWEVER THE SAME MAY BE CAUSED, INCLUDING FAULT OR NEGLIGENCE OF THE PARTY. FOR PURPOSES OF THIS AGREEMENT, COSTS OF DATA RECOVERY DUE TO A SOFTWARE OR SERVICE FAILURE AND COSTS TO RESPOND TO A SECURITY BREACH SHALL BE CONSIDERED DIRECT DAMAGES EXCEPT WITH RESPECT TO CLAIMS RELATED TO BREACH OF CONFIDENTIALITY, BREACH OF SECURITY, IP INFRINGEMENT OR INDEMNIFICATION FOR THIRD PARTY CLAIMS, IN NO EVENT SHALL EITHER PARTY'S LIABILITY TO THE OTHER UNDER OR IN RESPECT OF THIS AGREEMENT EXCEED \$1,000,000.
- (O) Mutual Negotiation. The Parties agree that the terms and conditions of this Agreement are the result of negotiations between the Parties and that this Agreement shall not be construed in favor of or against any Party by reason of the extent to which any Party or its professional advisors participated in the preparation of this Agreement.

- (P) Survival. Those provisions of this Agreement that would require survival in order to give them full force and effect shall survive the termination or expiration of the Agreement, regardless of the date, cause or manner of such termination
- (Q) Further Assurances. Each of the parties hereto shall execute and deliver any and all additional papers, documents and other assurances, and shall do any and all acts and things reasonably necessary in connection with the performance of their obligations hereunder to carry out the intent of the parties hereto.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the date first above written.

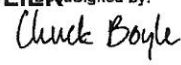
TE CONNECTIVITY CORPORATION

By: 

Name: John S. Jenkins, Jr.

Title: EVP & General Counsel

SUPPLIER Signed by:

By: 

Name: Chuck Boyle

Title: Chief Financial officer

Appendix A – Exhibit on Processing of Personal Information

Appendix B – Support Service Levels

Appendix C – Master Statement of Work

APPENDIX A

Processing of Personal Information

This Appendix A, Processing of Personal Information must be completed when required based on article 5 (D) (1) of the Agreement and when TE and Supplier conclude that no alternative solutions to comply with legal restrictions on the transfer of personal information are available.

In order to comply with these restrictions, the following Standard Contractual Clauses form an integral part of the Agreement. TE Connectivity Corporation signs these Standard Contractual Clauses on behalf of itself and its global affiliates.

Standard Contractual Clauses (data processing agreement)

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC on the protection of personal data, for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: TE Connectivity Corporation, a Pennsylvania Corporation, on behalf of itself and its global affiliates, see the most current list below the website privacy policy on www.te.com, a TE Connectivity Ltd. company, with offices located at 1050 Westlakes Drive, Berwyn, PA, USA, 19312 ("TE"); privacyoffice@te.com

Other information needed to identify the organisation:.....

.....
(the data **exporter**)

And

Name of the data importing organisation:

Other information needed to identify the organisation:

.....
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

*Clause 2****Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3****Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4****Obligations of the data exporter***

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer²

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and

² Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
 - (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
 - (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
 - (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
 - (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
 - (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
 - (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
 - (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal

obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9***Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10***Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11***Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses³. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established. See for this the front page.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority. -----

³ This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

*Clause 12****Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): Joe Eckroth -----

Position: SVP, CIO

Address: 1050 Westlakes Drive, Berwyn, PA, USA, 19312

Date:-----

Other information necessary in order for the contract to be binding (if any): -----

Signature.....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Chuck Boyle

Position: CFO-----

Address: 929 Broadway, Denver, CO 80203

Date:-----

Other information necessary in order for the contract to be binding (if any):

Signature.....

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporters are affiliates of TE Connectivity Corporation ("TE Connectivity") that is developing, producing and distributing a large number of electronic products and components globally. The data exporter wants to make use of a range of information technology and data processing services required for operating its business which services TE Connectivity is willing to provide, by itself and/or via subprocessors.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

a provider of a Software as a Service ("SaaS") cloud computing solutions for its clients ("data exporter" or "data controller") that processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement. If applicable to the data exporter's Agreement, employees of the data exporter can report incidents through an EU/Swiss equivalent to an 800 number or through the data importer SaaS application.-----

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The personal data transferred concern the following categories of data subjects (please specify):

Employees, officers, directors, vendors, contractors and other related or third parties working with or for data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

The personal data transferred concern the following categories of data (please specify):

Contact details (e.g., name, postal address, email address, and telephone number); Username and password for the account of data subjects may establish in our application; Photographs, videos, comments, and other content or information data subjects may submit to data importer through the application.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

The personal data transferred concern the following special categories of data (please specify):

Although the data importer has advised the data exporter against including any sensitive data in the personal data that is transferred, reporting individuals can include any information they choose. The data exporter controls such data in its sole discretion. **Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

The personal data transferred will be subject to the following basic processing activities (please specify):

Personal data may be transferred through a third party hosted cloud environment, through data importer's call center if submitted telephonically or through SFTP or API protocols. All transfers shall be in accordance with the Agreement.

DATA EXPORTER

Name:

Date:

Authorised Signature

DATA IMPORTER

Name:

Date:

Authorised Signature:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached): – see also the Data Privacy Questionnaire for this project as completed by both Parties and attached to this Appendix 3:

1. Physical Access control (to data processing systems):

Measures to prevent unauthorised persons from obtaining physical access to the data processing systems with which personal data are processed.

- The data center buildings are controlled by Azure and Amazon Web Services. Both partners are ISO 27001 and SOC 2 Certified

2. Access control (to use of data processing systems and methods):

Measures to prevent data processing systems and methods from being used by unauthorised persons.

- Complex passwords are enforced with system policy and expiration times appropriate to the level of access. Privileged accounts have more stringent controls including short life passwords with enterprise level management
- Accounts are locked for invalid attempts to log on and audit trails are logged and monitored for inappropriate and un-authorized activity
- Role based authentication is used where possible with auditing processes and activities to manage appropriateness of access. Privileged accounts utilize two-factor authentication with enterprise level management where required.
- Data systems are encrypted in transit using HTTPS and at rest using Microsoft SQL TDE.
- Strict Firewall rules are established only allowing required access to and from the production environment
- Internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data.
- The Data Importer designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access.
- These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. The granting or modification of access rights must also be in accordance with the Data Importer's internal data access

policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented.

3. Access control (to data):

Measures to ensure that persons who are authorised to use a data processing method only have access to that personal data to which their access authorisation applies and that this data cannot be read, copied, modified or removed during processing without authorization.

- User accounts are unique and assigned to appropriate groups by administrative personnel for control
- Roles limit access to objects through an authorization process with appropriate audit trails
- Audit logs are monitored for activity and access appropriateness
- System policies and procedures protect data during processing for appropriate access by authorized personnel
- All changes to access are logged and reviewed during periodic audits. Abnormal changes create alerts to appropriate personnel
- Data is deleted according to policy and wiped when no longer required

4. Disclosure controls:

Measures designed to ensure that personal data cannot be read, copied, modified or removed during electronic transmission, data transport or storage on data carriers without authorisation.

- Industry standard practices are employed to protect data in transit. Private Networks, Virtual Private Networks and Secure Socket Layer technologies are used to prevent unauthorized access
- Logging of system access is monitored and reviewed for appropriateness

5. Input controls:

Measures to ensure that it is possible to retroactively check and verify whether, when and by whom data has been entered into, modified or removed from the data processing system.

- Our access and activity logs are monitored and have alert triggers for unauthorized or inappropriate activity as well as provide change history

6. Control of instructions:

Measures to ensure that personal data are processed solely in accordance with the instructions of the Client.

- Corporate compliance and security policies highlight that client data is accessed only with a business need and is not disclosed

7. Availability control:

Measures to ensure that personal data are protected from accidental destruction or loss.

- Systems are backed up daily to enable recovery of data on a schedule determined by policy
- High availability or recovery technologies are employed to maintain system operation, availability and redundancy
- Production environments are replicated in geographically separated data centers with remote storage of backups and recovery systems
- Our infrastructure includes state-of-the-art firewall, anti-malware, and malicious activity detection technology
- Our Disaster Recovery Plans are documented, reviewed and tested on a regular basis

8. Separation controls:

Measures to ensure that personal data that is stored for separate purposes is processed separately.

- We have a tiered development, testing, stage and production environment to separate function and operation
- Access controls are employed to segregate the environments

9. Personnel:

- The Data Importer's personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The Data Importer conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
- Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer's confidentiality and privacy policies. Personnel are provided with security training.

10. Subprocessor Security:

- Prior to onboarding Subprocessors, the Data Importer conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

INDEMNIFICATION CLAUSE

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

- (a) the data exporter promptly notifying the data importer of a claim; and
- (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.

APPENDIX B Support Service Levels

Support Service Levels: During the Term of this Agreement, Supplier shall provide the support services described in this Appendix B.

"Support Service Levels" consist of: (i) providing telephone and email consultative support to TE's designated support personnel concerning the operation of the Hosted Software Service; and (ii) providing upgrades, updates, fixes, workarounds and error corrections to remedy errors.

Consultative Support: During the Term, TE's designated support personnel may contact Supplier to obtain telephone and email consultative support concerning the operation of the Hosted Software Service and to report errors. Supplier will designate a specific telephone number for TE's use for consultative support.

Response and Resolution Schedule: Supplier will classify each Error reported by TE based on the following criteria:

Error Classification	Criteria
Severity 1	Fatal: Errors that result in the loss of all promised capability.
Severity 2	Severe Impact: Errors which disable major functions from being performed and therefore affect the normal operation of the software during the normal working day.
Severity 3	Degraded Operations: Errors disabling only certain nonessential functions but do not affect the normal operation of the software during the normal working day.
Severity 4	Minimal Impact: Intermittent Errors affecting use of certain nonessential functions of the software.

Supplier shall respond to error reports during normal business hours (8am – 5pm MT, M-F, excluding Supplier observed holidays) according to the following schedule:

Error Classification	Acknowledge Receipt of Error Report	Provide a workaround, Fix or Documentation
Severity 1	1 hour	6 hours
Severity 2	1 hour	12 hours
Severity 3	8 hours	3 days
Severity 4	1 day	10 days, or as otherwise mutually determined

During the term of the Agreement, Supplier will install all upgrades, new releases, updates, releases, bug fixes, and enhancements thereto at no additional charge to TE.

Appendix C

MASTER STATEMENT OF WORK

PREMIUM IMPLEMENTATION

Convercent, Inc. ("Convercent" or "Supplier") and TE Connectivity Corporation ("Customer" or "TE") have entered into a Master Software as a Service (Hosting) Agreement, dated as of September 29, 2017 (the "Agreement"). This Master Statement of Work is made pursuant to the terms and conditions of the Agreement. In the event of an explicit conflict or inconsistency between the Agreement and this Master Statement of Work, the Agreement will control. Capitalized terms used but not otherwise defined herein shall have the meanings set forth in the Agreement or the applicable Description of Services.

As described herein, Convercent shall provide to Customer implementation services for the SaaS Products purchased by Customer pursuant to this Statement of Work and the Agreement. This Master Statement of Work Number ("Statement of Work") shall begin on the Effective Date of the Agreement and shall be coterminous with the term of the Agreement. Notwithstanding the foregoing, this Statement of Work will automatically terminate in the event either party duly terminates the Agreement.

In addition to any specific obligations set forth below, Customer and Convercent shall promptly respond to the other parties requests for information reasonably necessary for its performance of the obligations in this Statement of Work.

1. Strategy and Planning.

Prior to configuring the Product, Convercent will meet with Customer to understand its requirements and will then develop a Project Plan agreeable to both parties.

- 1.1. **Onsite Kickoff.** Convercent will provide one (1) eight (8) hour onsite kickoff session for designated Administrators and Moderators of the Product during October 2017. Convercent's dedicated transition team, including Scott Serrano, National Account Executive, Erin Dominguez, Customer Success Manager, and Autumn Sanelli, Global Solutions Director, will meet with TE primary points of contact during this onsite kickoff. The parties shall set, reasonably in advance, a mutually agreeable date for the onsite kickoff. The onsite kickoff will: provide team introductions; confirm goals, expectations and success criteria for implementation; confirm timing and project milestones; provide a project overview and approach; identify project resource requirements; discuss an approach to change management; provide product demonstrations and detailed discovery; and schedule planning and next steps.¹
- 1.2. **Project Plan.** Following the kick-off meeting Convercent will develop a detailed Project Plan for Customer's review and feedback and deliver the same to Customer. This process shall repeat, with Convercent revising the Project Plan following Customer's feedback, until a mutually agreeable Project Plan has been developed. The parties will then align resources in accordance with the Project Plan and Convercent will maintain the Project Plan as the parties move forward with implementation.
- 1.3. **Project Team.** Implementation will be provided by a dedicated Convercent transition team, including but not limited to the above identified individuals in Section 1.1 and a TE primary point of contact, and implementation expert who will continue to work with TE throughout this Agreement. Telephony expert; solutions support resource to guide data migration.
- 1.4 **Ongoing Support.**
 - 1.4.1 Onsite. The parties will establish the necessary frequency of additional onsite meetings, virtual meetings, etc. Additional onsite trainings would be available for an additional mutually agreeable fee.
 - 1.4.2 Remote. On request by Customer, the TE point of contact and Customer Success Manager will meet (which may include by electronic means, or remotely) to discuss and evaluate the Project Plan and each party's performance under this SOW No. 1 post go-live and during the deployment of the project.

¹ For the avoidance of doubt, all other training provided for under this Statement of Work will be provided remotely in a virtual environment. Any additional on-site training will require a separate statement of work at Convercent's then current fees.

- 1.4.3 Materials.** As part of the Premier Implementation, Convercent will provide Customer with access to an online portal with on-demand access to Convercent's complete library of product reference guides, searchable knowledge base, communication and rollout materials, workflows and templates in relation to the Service.

2. Configuration.

2.1. Technical Configuration.

- 2.1.1. Organization Setup.** Convercent will grant primary Administrators access to the Product and will provide detailed training on how to configure the Customer's specified organizational structure and settings.
- 2.1.2. SSO.** Access to the Product is restricted to Users by user name and password. If Customer has purchased SSO authentication services, Users may login through the Product or through Single Sign-On ("SSO"). Convercent will provide Customer with reasonable support to establish SSO authentication for all of Customer's Users. Support will include initial documentation and discovery questions provided to Customer technical resources, access to SSO resources from Convercent's solution support team, and availability of Convercent's solution support team to provide trouble-shooting on live calls.
- 2.1.3. Initial HRIS Data Upload.** Customer will provide Convercent with an HRIS file of Customer's personnel in a .csv file via secure file transfer (SFTP), with the data attributes agreed to in the Project Plan, in the format specified by Convercent. After receiving the initial HRIS file, Convercent will upload the data to the platform. If the file contains any errors or is not successfully uploaded, Convercent will send Customer a file listing the errors via the SFTP site. Customer will then resolve any errors, and send Convercent a revised file for uploading and Customer review. This process will continue until the HRIS file is accurately and completely uploaded. Following this initial upload, Convercent will accommodate an HRIS data update of any changes to Customer's workforce, and an ongoing HRIS data update cycle will begin at a cadence to be mutually agreed.

2.2. Hotline and Case Manager Configuration.

2.2.1. Case Manager.

- 2.2.1.1. Configuration.** The parties will work together to configure the Case Management Module to meet Customer's specifications in accordance with the details set forth in the Project Plan. As a general matter, either (i) Customer will configure the Case Management Module with Convercent's reasonable assistance, if needed, or (ii) provided that Customer has provided Convercent all required information in a Convercent approved format, Convercent will configure the Case Management Module pursuant to Customer's specifications. Regardless of the primarily responsible party, configuration of the Case Management Module to meet Customer's specifications will include defining organization names and general settings, selecting issue types, adding custom issue types (if purchased), configuring intake channels (including geography rules thereto), configuring employee groups, configuring Notification Profiles, and configuring Customer's Landing Page (and repointing an existing URL if necessary).
- 2.2.1.2. Testing.** Following the configuration set forth above, Convercent will advise Customer on an appropriate plan for testing the configurations in the Case Management Module. Customer will test the web intake by submitting reports to trigger various Routing rules and Notification Profiles, reviewing access levels to confirm which Users have access to which Cases, and confirming that the correct Users receive Alerts. Customer will test the report management functionality by updating different fields (e.g. locations, issue types, messages). If Customer determines there are issues with the configuration that need to be resolved, Customer will notify Convercent of the issue and Convercent will determine whether the issue is Product related or configuration related. Where the issue relates to the Product, Convercent will escalate the issue internally for resolution and request documentation regarding the issue from Customer as needed. Where the issue relates to configuration of the Product, Convercent will assist Customer with reconfiguring the Product to resolve the issue. In either instance, Customer will then re-test to confirm the Case Management Module materially conforms to the specified configurations. The configuration for the Case Management Module will include custom fields for TE's Security Team, Ombudsmen, Human Resources and other departments or personnel upon TE's reasonable request. For the avoidance of doubt, use of the Case Management Module by these groups is covered by the license detailed in Section V of the Agreement.

2.2.2. Hotline.

- 2.2.2.1. Configuration.** Convercent will configure the Hotline as agreed upon in the Project Plan, in accordance with one of the three methods below. For each method below, provided that Customer has provided

the required information in Convercent specified format, Convercent will record standard hotline greetings in Customer's specified languages for each new phone number and configure the Hotline interactive voice response ("IVR") capability.

Shared Lines. Where the parties agree to utilize Convercent's shared lines, Customer's Hotline will be directed thereto. Shared lines are pre-configured and ready to use.

Dedicated Lines. Where the parties agree to provide dedicated lines for Customer, Convercent will procure and host the number of audio bridges purchased by Customer, each of which shall be pointed to Convercent's call center.

Existing numbers. Where the parties agree to re-point Customer's existing Customer-owned Hotline number to Convercent's call center via direct inward dialing, Convercent will provide reasonable assistance, if needed.

2.2.2.2. **Testing.** Convercent will supply Customer with a testing template, which Customer will utilize to test the Hotline and identify any issues. Prior to the Hotline going into production, Customer will call the Hotline direct (from different countries if necessary) to test its functionality and assure that it functions in accordance with the custom greetings Customer has provided (during configuration) and that there are no connection issues. If Customer determines there are issues with the configuration that need to be resolved, Customer will notify Convercent of the issue and Convercent will modify greetings and/or IVR accordingly. Customer will then re-test to confirm the Case Management Module materially conforms to the specified configurations.

2.3. **Data Migration.** Customer historic data will be mapped to a Convercent template (by either Convercent or Customer, as mutually agreed) and Convercent will upload the same to the Case Management Module. The specifics of this process will be set forth in detail in the Project Plan and vary by customer, and the below is solely a general overview of the process.

2.3.1. The Convercent Data Migration team will be comprised of a Solutions Support Specialist who will be responsible for analyzing TE's historical data and mapping that data to existing Convercent fields and led by the Customer Success Manager. After the initial mapping, Convercent will set up follow-up meetings to review the mapping for TE to determine next steps.

2.3.2. **Conditions precedent to data mapping.** Before Convercent can map Customer's historic data, Customer must (A) upload the data to the Convercent SFTP site, (B) if applicable, provide Convercent a .csv or .xml file of its HRIS data in a format specified by Convercent, (C) if applicable, provide Convercent its desired custom fields and (D) if applicable, provide Convercent its desired custom issue types.

2.3.3. Upon Customer's completion of the conditions precedent indicated above, the data mapping and upload process will be as follows:

- (i) Convercent will map Customer's historic data fields to Convercent fields;
- (ii) Customer will review the accuracy of the mapped data, and note any errors;
- (iii) Convercent will re-map the data as necessary and steps (i) through (iii) shall repeat until the mapped data materially conforms to Customer's specifications;
- (iv) Convercent will upload the mapped data to a trial environment;
- (v) Customer will review the data in the trial environment for accuracy and note any errors;
- (vi) Convercent will resolve errors and re-upload the data; steps (iv) through (vi) shall repeat until the uploaded data materially conforms to Customer's specifications;
- (vii) Convercent will upload the fully mapped historic data to Customer's production environment.

3. **Product Training.**

3.1. Convercent shall provide appropriate product training for Customer personnel who serve as Administrators and Moderators of the Case Management Module, based on a "train the trainer" approach. This training will include up to three (3) remote training sessions. The remote training sessions will train on items requested by Customer relating to the Product and best User practices including but not limited to the Product functionality.

3.2. In addition to the onsite kickoff referenced above, Convercent shall provide recorded trainings for primary administrators and case managers. Additionally, Convercent will support reasonably requested trainings throughout the contract term, but the expectation is that trainings will be provided on a group basis, not a one-off. Furthermore, Convercent provides weekly recorded trainings, with a Convercent representative to answer questions, and access

to support portal discussed in section 1.4.3 above, inclusive of knowledge base articles, how to videos, customizable training templates, configuration workbooks and testing templates. All training resources, including onsite and virtual, are available throughout the Term, and shall be made fully available for TE's use no later than January 1, 2018.

4. Communication and Rollout.

- 4.1. **Strategy and Resources.** Convercent will work with Customer to develop a strategy to communicate product launch to internal stakeholders. Customer will determine how to announce the Convercent Services to its employees via the method it deems appropriate. Customer has the option to purchase finished communication material from Convercent, utilize Convercent sample templates (which are provided with Customer's purchase of the Services), or use Customer's own marketing resources to build its own communication material.
- 4.2. **Rollout.** Once Customer determines the appropriate communication strategy and develops its desired communication materials to implement that strategy, Customer will launch the Services by providing an official communication to its employees. For clarity, the Services will be available to Customer administrative users following configuration and testing, and the launch will consist solely of Customer's communication to Customer its employee base that they may now submit Reports via the Convercent Products and Services

5. General Timeframe.

The timeline below provides the milestones the parties will meet in this implementation; the means of reaching these milestones shall be more fully detailed in the Project Plan.

- 5.1. By November 1, 2017, TE shall provide Supplier with: (A) a data set comprised of all closed cases, from its existing vendor ("Data Set 1"), uploaded to Supplier's SFTP site, (B) a .csv file of its HRIS data in a format reasonably specified in advance by Convercent, and (C) its desired custom fields and (D) its detailed custom issue types, and ancillary reporting formats to support TE's security Team Ombudsman and the HR functions as needed.
- 5.2. By January 1, 2018, Convercent shall provide TE with (A) a configured production environment within the Case Management Module; (B) fields necessary within the Case Management Module to allow for data mapping, and (C) fully functional and operational telephony services.
- 5.3. By January 2, 2018, TE shall request a data set comprised of all remaining cases from its existing vendor ("Data Set 2"), and shall upload Data Set 2 to Supplier's SFTP site as soon as reasonably practicable.
- 5.4. Within ten (10) days following receipt of Data Set 2 uploaded to Supplier's SFTP site, Supplier shall load the same, accurately mapped, into the Case Management Module's production environment.
- 5.5. By March 1, 2018, Convercent shall upload Data Set 1, accurately mapped, to the Case Management Module's production environment.

This section intentionally left blank

Sample Project Plan

team member
team member

team member
team member

Date	Milestone
Date	Milestone
Date	Milestone

	Assigned To	Status	% Complete	Due Date	Notes
Project kickoff meeting					
Team introductions		●	○		
Confirm goals, expectations and success criteria		●	○		
Confirm timing and project milestones		●	○		
Project overview and approach		●	○		
Identify project resource requirements		●	○		
Discuss change management approach					
Schedule planning and next steps		●	○		
Requirements definition					
Hotline and Case Management					
Confirm intake methods and and case management systems		●	○		
Confirm locations, organizational units, employees		●	○		
Confirm international data privacy requirements		●	○		
Confirm language requirements		●	○		
Confirm user access rights, roles, permission requirements		●	○		
Confirm intake channel requirements		●	○		
Confirm notification profile requirements		●	○		
Confirm landing page requirements		●	○		
Campaigns					
Confirm audience/employees that will receive campaigns		●	○		
Confirm use case (i.e. new hire onboarding, code of conduct, etc)		●	○		
Confirm campaign timing needs and frequency		●	○		
Confirm if campaigns will include policies and/or learning		●	○		
Confirm availability of content required for campaigns		●	○		
Conflicts of Interest					
Confirm audience/employees that will be required to disclose COIs		●	○		
Confirm use case and current disclosure process		●	○		
Confirm if any COI intake form customizations are required		●	○		
Confirm timing needs and frequency		●	○		
HR data import					
Confirm HR data import requirements		●	○		
Confirm candence for ongoing HR data updates		●	○		
Telephony (for Hotline and Case Management)					
Confirm use cases		●	○		
Confirm hotline toll-free number requirements		●	○		
Confirm language translation requirements		●	○		
Confirm hotline custom greeting requirements		●	○		
Define plan for migrating hotline services from current provider, if required		●	○		
Legacy data migration (for Hotline and Case Management)					
Confirm process and timing		●	○		
Confirm data mapping needs		●	○		
Reporting					
Define reporting needs and use cases		●	○		
Define plan for custom report development (if required)		●	○		
Training and rollout requirements					
Define training needs, process and timing		●	○		
Define resource needs		●	○		
Define communication strategy		●	○		
Define rollout strategy		●	○		
Project Plan					
Define change management strategy		●	○		
Develop detailed project plan		●	○		
Team review and signoff on project plan		●	○		

	Assigned To	Status	% Complete	Due Date	Notes
Product configuration training					
Create organization in Convercent		<div><div></div></div>	<div><div></div></div>		
Set up user records for configuration administrators		<div><div></div></div>	<div><div></div></div>		
Conduct product configuration training for administrators		<div><div></div></div>	<div><div></div></div>		
Product configuration					
Define organization alias names and general settings		<div><div></div></div>	<div><div></div></div>		
Hotline and Case Management					
Select issue types, if required for guided intake		<div><div></div></div>	<div><div></div></div>		
Configure intake channels		<div><div></div></div>	<div><div></div></div>		
Configure notification profiles		<div><div></div></div>	<div><div></div></div>		
Configure intake channel geography rules		<div><div></div></div>	<div><div></div></div>		
Configure landing page		<div><div></div></div>	<div><div></div></div>		
Configure employee groups (if required)		<div><div></div></div>	<div><div></div></div>		
Campaigns					

Phase 3 - Product Training

		Assigned To	Status	% Complete	Due Date	Notes
--	--	-------------	--------	------------	----------	-------

[illegible]

		Assigned To	Status	% Complete	Due Date	Notes
--	--	-------------	--------	------------	----------	-------

[illegible]
